

### **Remarks and Arguments**

Claims 1-11, 17-20 and 28-37 have been presented for examination. Claim 35 has been amended.

Claims 1-2, 4-5, 6-11, 17-18, 20 and 34-37 have been rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,564,320 (de Silva, previously cited) in view of U.S. Patent No. 6,671,804 (Kent.)

As previously discussed, in the present invention, the registration authority sends both the request and its identifier to the certificate authority so that the identifier can be included in the certificate. The registration authority identifier allows the registration authority associated with the certificate to be quickly identified so that certificates associated with that registration authority can later be efficiency revoked.

In the de Silva patent the local server generates the request, as noted by the examiner, and corresponds to the recited registration authority. The examiner admits that the de Silva patent does not disclose that the certificate generated by the certificate authority includes any information identifying the local server (202). However, the examiner claims that the Kent patent discloses a certificate that contains an identifier of a registration authority.

The Kent patent discloses a template database that allows a cryptographic module to operate with more than one registration authority. In particular, templates can be “bound” to one or more registration authorities by including information in the database that identifies the registration authorities associated with a template. Each template includes the syntax of certificates and certificate requests generated by the authorities to which the template is bound. When a certificate request is sent to the cryptographic module, the module uses a registration authority identifier in the request to retrieve the associated template which is then used to check the syntax of the request and certificate sent by the registration authority.

The Kent patent discloses that a template can include fields and extension fields in the X.509 v.3 public key certificate specification. These fields include authority and subject key identifiers, key usage restrictions, certificate policies, policy mappings and issuer and subject alternate names. However, the X.509 v.3 specification does not include a field or field extension for a registration authority identifier.

The Kent patent also discloses that the templates can include private field extensions. The examiner claims that the Kent patent discloses that such a private extension could include a registration authority identifier, pointing to Kent, column 7, lines 36-62. At the specified location, Kent discusses supporting multiple authorities by binding them to a template by including the authority identifiers in a rules database. The patent also discloses that extension fields in the template can be used to support changes that might occur in the system. At lines 53-62, Kent states that, in a situation where a new software application is deployed and a specific registration authority designated to issue certificates that constrain the use of the new application, “a new extension in an X.509 certificate specific to the new application may be created and stored in a template 310 to identify this particular RA as the point of contact for issuing the certificates required to use the new application.”

Applicant does not believe that this statement would be interpreted by those skilled in the art as a teaching that a certificate should or could include a registration authority identifier. Read literally, the statement indicates that the field extension in a template is related to the new software application rather than the registration authority. This is particularly so because, in this section, Kent specifically teaches that a template is associated with a particular registration authority by binding that template to the registration authority with the rules database, not by including a registration authority identifier in the certificate. It is only after reading the disclosure of the present invention that the interpretation urged by the examiner might become apparent.

Thus, neither the de Silva patent nor the Kent patent disclose including a registration authority identifier in a certificate. Thus, the proposed combination of these references cannot teach this feature. The general motivation of better protecting information from unauthorized usage posited by the examiner cannot serve as the specific motivation for interpreting a sentence in Kent to encompass a teaching that is not supported by the surrounding context.

The present claims specifically state that the issued certificate includes an identifier of the requesting registration authority. Claim 1 is illustrative. It recites, at lines 8-12 that the certificate “...request includes a first identifier that identifies the registration authority; and at the certification authority in response to receipt of the

request, generating a certificate that includes said first identifier.” As discussed above, neither de Silva nor Kent discloses such a certificate. Therefore, claim 1 patentably distinguishes over the cited reference combination.

Claims 2, 4-5 and 6-11 are dependent, either directly or indirectly, on claim 1 and incorporate the limitations thereof. Therefore, they distinguish over the cited combination of references in the same manner as claim 1. In addition, these claims recite limitations not taught or suggested by the cited combination of references. For example, claim 7 recites that the certificate includes a time stamp associated with the request. The examiner admits that the proposed combination of de Silva and Kent does not specifically disclose a time stamp associated with the request, but claims that the recited timestamp is still obvious. Since there is no teaching in the proposed combination, in order to establish *prima facie* obviousness, the references must suggest the claimed feature. However, for this suggestion, the examiner has provided only the general motivation of allowing the system to more securely track each transaction. This general motivation cannot suggest the specific modification as claimed. Thus, the combination of de Silva and Kent does not establish *prima facie* obviousness and consequently this rejection is respectfully traversed by Applicant. See MPEP §2143.03

Claim 17 distinguishes over the cited combination in the same manner as claim 1. For example, claim 17 recites, in lines 6-10, “receiving a request from a registration authority to issue a certificate on behalf of a principal; and in response to receipt of said request, generating said certificate that includes at least a registration authority identifier associated with said registration authority.” As discussed above, neither de Silva nor Kent discloses that a generated certificate include an identifier associated with a server that might correspond to the recited “registration authority”. Nor can the combination of these references suggest this recited combination also as discussed above. Thus, claim 17 patentably distinguishes over the cited combination of references.

Claims 18 and 20 are dependent on claim 17 and incorporate the limitations thereof. Therefore, they distinguish over the cited combination of references in the same manner as claim 17. In addition, these claims recite limitations not taught or suggested by the cited combination of references. For example, claim 20 recites that the certificate includes a timestamp associated with the request in a manner similar to

claim 7. Therefore, claim 20 distinguishes over the cited combination of references in the same manner as claim 7.

Claim 34 contains limitations that parallel those in claims 1 and 17 and distinguishes over the cited combination of references in the same manner as claims 1 and 17. Claims 35-37 are dependent on claim 34 and incorporate the limitations thereof. Therefore, they distinguish over the cited combination of references in the same manner as claim 34. In addition, these claims recite limitations not taught or suggested by the cited combination of references. For example, claim 37 recites a means that provides an indication that a certificate is untrustworthy based on a comparison of a node identifier in the certificate with the node identifier of an untrustworthy node on a certificate revocation list. The examiner points to de Silva as disclosing revocation of certificates. However, de Silva does not disclose how the certificates are revoked as recited in claim 37. Consequently, de Silva does not disclose the limitations in claim 37 and claim 37 patentably distinguishes over de Silva and Kent.

Claims 3, 19 and 28-33 have been rejected under 35 U.S.C. §103(a) over de Silva in view of Kent and further in view of U.S. Patent No. 6,308,277 (Vaeth, previously cited.) Claim 3 is dependent on claim 1 and incorporates the limitations thereof. This claim distinguishes over the combination of de Silva and Kent as discussed above. Adding Vaeth to the combination does not supply the limitations that are missing in the combination of de Silva and Kent. In particular, Vaeth discloses a certification system that includes a registration authority and a certificate authority. However, as discussed in the immediately preceding responses, Vaeth does not disclose or suggest that the registration authority, which makes the certificate request to the certificate authority, makes a certificate request which includes an identifier identifying the registration authority as recited in claim 1. Therefore, the certificate returned to by the certificate authority does not include this identifier also as recited in claim 1. Consequently, claim 3 distinguishes over the cited combination in the same manner as claim 1.

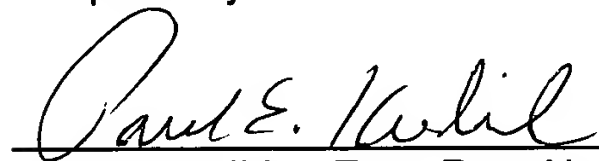
In the same manner, claim 19 is dependent on claim 17. As discussed above, claim 17 distinguishes over the cited de Silva and Kent combination. Since adding the

Vaeth reference to this latter combination does not change the combination such that it would render claim 17 obvious, claim 19 also distinguishes over the cited combination.

Claim 28 recites "program code ... for generating by a certification authority a certificate ... includes ... a registration identifier associated with said registration authority." Thus, claim 28 patentably distinguishes over the cited combination of de Silva and Kent as discussed above with respect to claim 1. Also as discussed above Vaeth does not teach such a certificate and thus cannot add what is missing in the de Silva and Kent combination. Thus, claim 28 patentably distinguishes over the cited reference combination. Claim 29 depends on claim 28 and, therefore, incorporates the limitations of claim 28 and patentably distinguishes over the cited combination in the same manner as claim 28. Claim 30 contains limitations that parallel those in claim 28 and distinguishes in the same manner. Claims 31-33 depend on and incorporate the limitations of claim 30 and thus distinguish over the cited combination in the same manner as claim 30.

In light of the forgoing amendments and remarks, this application is now believed in condition for allowance and a notice of allowance is earnestly solicited. If the examiner has any further questions regarding this amendment, she is invited to call applicants' attorney at the number listed below. The examiner is hereby authorized to charge any fees or direct any payment under 37 C.F.R. §§1.17, 1.16 to Deposit Account number 02-3038.

Respectfully submitted



Date: 3/13/06

Paul E. Kudirka, Esq. Reg. No. 26,931  
KUDIRKA & JOBSE, LLP  
Customer Number 045774  
Tel: (617) 367-4600 Fax: (617) 367-4656